EXP MAIL: EL533648746US 520 Rec'd PCT/PTO 03 DEC 1999

FORM PTO-1390 (Modified) (REV 10-95) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER: RCA88674

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR): 09/445133

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US98/11634	05 June 1998	06 June 1997

TITLE OF INVENTION
GLOBAL CONDITIONAL ACCESS SYSTEM FOR BROADCAST SERVICES

APPLICANT(S) FOR DO/EO/US
Ahmet Mursit Eskicioglu

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ A copy of the International Search Report (PCT/ISA/210).
8. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
9. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 18 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98. w/5 refs + PCT Search Rept.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
    A **SECOND** or **SUBSEQUENT** preliminary amendment.
16. ☐ A substitute specification.
17. ☐ A change of power of attorney and/or address letter.
18. ☒ Certificate of Mailing by Express Mail
19. ☒ Other items or information: Return Receipt Postcard

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/445133	PCT/US98/11634	RCA88674

20. The following fees are submitted:	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :		
☒ Search Report has been prepared by the EPO or JPO	$840.00	
☐ International preliminary examination fee paid to USPTO (37 CFR 1.482)	$670.00	
☐ No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2))	$760.00	
☐ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO	$970.00	
☐ International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4)	$96.00	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$840.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).	$0.00	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	20 - 20 =	0	x $18.00	$0.00	
Independent claims	3 - 3 =	0	x $78.00	$0.00	
Multiple Dependent Claims **(check if applicable)**.			☐	$0.00	
TOTAL OF ABOVE CALCULATIONS			=	$840.00	
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) **(check if applicable)**.			☐	$0.00	
SUBTOTAL			=	$840.00	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)).			+	$0.00	
TOTAL NATIONAL FEE			=	$840.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).**			☐	$0.00	
TOTAL FEES ENCLOSED			=	$840.00	
				Amount to be: refunded	$
				charged	$

☐ A check in the amount of to cover the above fees is enclosed.

☒ Please charge my Deposit Account No. **07-0832** in the amount of **$840.00** to cover the above fees.
A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **07-0832** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Joseph S. Tripoli - Patent Operations
Thomson multimedia Licensing Inc.
PO Box 5312, 2 Independence Way
Princeton, NJ 08543-5312

SIGNATURE

David T. Shoneman
NAME

39,371
REGISTRATION NUMBER

12/3/99
DATE

EXP. MAIL: EL533648746US

09/445133 RCA88674

418 Rec'd PCT/PTO 0 3 DEC 1999

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	: Ahmet Mursit Eskicioglu
Int'l. Appl. No.	: PCT/US98/11634
Int'l. Filing No	: 05 June 1998 (05.06.98)
For	: GLOBAL CONDITIONAL ACCESS SYSTEM FOR BROADCAST SERVICES

PRELIMINARY AMENDMENT

Honorable Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

In the US national phase application of PCT/US98/11634 filed herewith, please enter the following amendments:

Please amend the claims as follows:

In the Claims

1. (Amended) A method for managing access to **a scrambled** [an] event of a service provider, said method comprising:

(a) receiving in a device an electronic list of events**, at least one event having an encrypted message associated therewith** [from a list provider, said list having a digitally signed message corresponding to each event in said list, each of said digitally signed messages comprise a message encrypted using a second public key and a digital signature created using a first private key];

[(b) selecting an event from said list;]

(b)[(c)]receiving in said device**, in response to user selection of said event,** said [digitally signed] **encrypted** message [corresponding to the selected event];

[(d) authenticating said list provider, using a first public key, in response to said digital signature];

(c)[(e)]decrypting said **encrypted** message [using a second private key] to obtain **a descrambling** [an event] key;

(d)[(f)]receiving [from the service provider] said selected event **from the service provider**, said selected event being scrambled using said **descrambling** [event] key; and

(e)[(g)]descrambling said selected event using said **descrambling** [event] key [to provide a descrambled event].

2. (Amended) The method of Claim 1 wherein the steps of decrypting said message, receiving said selected event, and descrambling said selected event are performed in a smart card coupled to the device, said **message being encrypted using a public key** [second private and public keys being] associated with said smart card and **said step of decrypting uses a private key associated with and** [said second private key being] stored in said smart card.

3. (Amended) The method of Claim 2 wherein said message further comprises event information, said event information being decrypted using said [second] private key.

4. (Amended) The method of Claim 3 further comprising the step of storing said event information, wherein said step of storing said event information is performed in said [removable] smart card.

6. (Amended) The method of Claim 5 **further comprising** [wherein the step of] authenticating **said list of events** [comprises decrypting said digital signature in said device] to verify the origin of said message.

7. (Amended) The method of Claim 6 wherein **each message further comprises a digital signature created using a second private key and the step of authenticating comprises decrypting said digital signature using a** [said first] **second** public key **that** is stored in said device.

10. (Amended) The method of Claim **7** [1] wherein said digital signature, said **second** [first] public key and said **second** [first] private key are issued by an independent certificate authority and are associated with said list provider.

15. (Amended) A method for managing access between a device having a smart card coupled thereto and a service provider, said device performing the steps of:

(a) receiving an electronic program guide from a guide provider, said guide having [a digitally signed message corresponding to each event in said guide, each of said digitally signed messages comprise] a message **and a digital signature associated with each event in said guide, said message being** encrypted using a public key of the smart card and **said** [a] digital signature **being** created using a private key of said guide provider;

(b) selecting an event from said guide;

(c) receiving said [digitally signed] **encrypted** message **and said digital signature** corresponding to the selected event;

(d) authenticating said guide provider by decrypting said digital signature using a public key of said guide provider, said guide public key being stored in said device;

(e) passing said message to **said** [a] smart card [coupled to the device];

(f) decrypting**, in said smart card,** said message using a private key of **said** [the] smart card to obtain event information and a symmetric key, said smart card private key being stored within **said** [the] smart card;

(g) storing said event information in **said** [the] smart card and updating account information based on said event information;

(h) receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and

(i) descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event.

18. (Amended) A method for managing access between a device having a smart card coupled thereto and a service provider, said device performing the steps of:

(a) receiving an electronic program guide **from a guide provider**, said guide having a digital certificate and a separate message corresponding to each event in said guide, each of said digital certificates being encrypted using a first private key of said guide, said separate message being encrypted using a public key of the smart card and having an associated digital signature created using a second private key of said guide;

(b) selecting an event from said guide;

(c) receiving said digital certificate, said message and said digital signature corresponding to the selected event;

(d) authenticating said guide provider by decrypting said digital certificate using a first public key of said guide to obtain a second public key of said guide, and

decrypting said digital signature using said second guide public key, said first guide public key being stored in the device;

(e) passing said message to said smart card;

(f) decrypting, **in said smart card,** said message using a private key of the smart card to obtain event information and a symmetric key, said smart card private key being stored within the smart card;

(g) storing said event information in the smart card and updating account information based on said event information;

(h) receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and

(i) descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event.

REMARKS

No fee is believed to been incurred by virtue of this amendment. However, if a fee is incurred on the basis of this amendment, please charge such fee against deposit account 07-0832.

Respectfully Submitted,
Ahmet Mursit Eskicioglu

By: 
David T. Shoneman, Attorney
Registration No. 39,371
(609) 734-9875

THOMSON multimedia Licensing Inc.
PO Box 5312, 2 Independence Way
Princeton, NJ 08543-5312

GLOBAL CONDITIONAL ACCESS SYSTEM FOR BROADCAST SERVICES

Field of the Invention

This invention concerns a system for providing conditional access (i.e., managing access) to a consumer electronic device, such as a set-top box or a digital television, that is capable of receiving broadcast digital streams from a variety of sources, such as, broadcast television networks, cable television networks, digital satellite systems, internet service providers and sources of electronic list of events.

Background of the Invention

Today, as depicted in Figure 1, a user may receive services from a variety of service providers, such as broadcast television networks 22, cable television networks 24, digital satellite systems 26, and internet service providers 28. System 10 of Figure 1 defines the present configuration for receiving services from such service providers. Most television receivers 12 are capable of receiving unscrambled, information or programs directly from broadcast and cable networks. Cable networks providing scrambled or encrypted programs usually require a separate stand-alone device 16a, 16b (e.g., a set-top box) to descramble or decrypt the program. Similarly, digital satellite systems usually provide scrambled or encrypted programs that also require the use of a separate set-top box. These set-top boxes may utilize a removable smart card 18a, 18b which contain the necessary decrypting algorithms and keys. Typically, a separate set-top box is required for each service

provider. Connections to the internet or world-wide web (web) are usually handled via a personal computer 14, or the like, and a modem 20. Traditionally, access to the internet is managed using a specially designed software package loaded onto the computer; this software enables a user to connect to an internet service provider who acts as the gate keeper to the web. The user typically pays a monthly fee to the service provider for access to the internet, either on a limited or unlimited basis. As one would expect there are numerous service providers, each which requires specialized software for access.

United States Patent Application Number US 5,592,551 teaches the transmission of lists of events (or program guides). European Patent Application Number EP-A-0 719 045 teaches a crypt key system in which the user provides the key necessary for decrypting to the broadcasting station. Particularly, the broadcasting station 11 broadcasts a public-key Kbd or a public-key pair using the scanning lines during the retrace blanking interval period of an analog television picture (col. 8, lines 50-58). The user sends a message comprising its secret key Ksu encrypted by the received public-key Kbd (col. 9, lines 14-25). The user's secret key Ksu is obtained using the corresponding private-key Kvd (col. 9, lines 26-30). The requested program is encrypted using the user's secret key Ksu, and then transmitted to the user via communication apparatus 15 and communication line 17 where it is decrypted using Ksu (col. 9, lines 31-44).

Summary of the Invention

The manufacturers of these digital televisions and set-top boxes may desire that they be compensated by the service provider for each connection to the service emanating from the box. Thus, the flexibility of open hardware architecture of the televisions and the set-top boxes in combination with a competitive market for such devices necessitates the need to provide a system for managing access so that the manufacturer is compensated for any use of its hardware to access any selected service provider. This invention resides, in part, in recognition of the described problem and, in part, in providing a solution to the problem.

An event or program as described herein comprises one of the following: (1) audio/visual data such as a movie, weekly "television" show or a documentary; (2) textual data such as an electronic magazine, paper, or weather news; (3) computer software; (4) binary data such as images or (5) HTML data (e.g., web pages). These service providers include any provider broadcasting events, for example,

traditional broadcast television networks, cable networks, digital satellite networks, providers of electronic list of events, such as electronic program guide providers, and in certain cases internet service providers.

Generally, the present invention defines a method for providing conditional access to a broadcast event from a service provider. That is, this method comprises receiving an electronic list of events, such as an electronic program guide, from a list provider, wherein the list has a digitally signed message corresponding to each event of the list or guide, the digitally signed message comprises a message encrypted using a second public key and a digital signature created using a first private key. The method further comprises selecting an event from the list; receiving the digitally signed message corresponding to the selected event; authenticating the list provider; decrypting the message using a second private key to obtain an event key; receiving the selected event which is scrambled using the event key; and descrambling the selected event using the event key to provide a descrambled event.

In accordance with one aspect of the present invention, the steps of decrypting the message, receiving the selected event, and descrambling the selected event are performed in a removable smart card coupled to the device wherein the second private key is stored in the smart card.

In accordance with another aspect of the present invention, the message comprises event information which can be decrypted using the second private key. The event information further being

stored in the smart card having a card body with a plurality of terminals arranged on a surface of the card body in accordance with one of ISO standard 7816 or PCMCIA card standards.

In accordance with yet another aspect of the present invention, a system for managing conditional access between a service provider and a device having a smart card coupled thereto, the device performing the steps of: receiving an electronic program guide having a digitally signed message corresponding to each event in the guide wherein each digitally signed message comprises a message encrypted using a smart card public key and a digital signature created using a guide provider private key; selecting an event from the guide; receiving the digitally signed message corresponding to the selected event; authenticating the guide provider by decrypting the digital signature; passing the message to a smart card; decrypting the message to obtain event information and a symmetric key; storing the event information in the smart card and updating account information; receiving the selected event which is scrambled using the symmetric key; and descrambling the selected event using the symmetric key to generate a descrambled event.

In accordance with yet another aspect of the present invention, a system for managing access between a service provider and a device having a smart card coupled thereto, the device performing the steps of: receiving an electronic program guide having a digital certificate and a separate message corresponding to each event in the guide, each of the digital certificates being encrypted using a first guide private key, the separate messages being encrypted using a smart card public key and containing an associated signature created

using a second guide private key; selecting an event from the guide; receiving the digital certificate, message and associated digital signature corresponding to the selected event; authenticating the guide provider; passing the message to a smart card; decrypting the message using a smart card private key to obtain event information and a symmetric key; storing the event information in the smart card and updating account information based on the event information; receiving the selected event wherein the selected event is scrambled using the symmetric key; and descrambling the selected event using the symmetric key to generate a descrambled event.

These and other aspects of the invention will be explained with reference to a preferred embodiment of the invention shown in the accompanying Drawings.

Brief Description of the Drawing

Figure 1 is a block diagram illustrating a prior art configuration for interconnecting consumer electronic devices to a variety of service providers.

Figure 2 is a block diagram illustrating one architecture for interfacing a common set-top box to a variety of service providers.

Figure 3 is a block diagram of an exemplary implementation of a system for managing access to a device in accordance with the invention; and

Figure 4 is a block diagram of another exemplary implementation of the system of Figure 3.

Detailed Description of the Drawing

The present invention provides a conditional access system which may be utilized to obtain services from one of a plurality of sources. The conditional access system when implemented within a set-top box permits the set-top box to authenticate the service provider before a broadcast event is purchased and uses a smart card for decrypting the encrypted event received from the service provider. Alternately, the functionality of the smart card may be embedded within the set-top box. Such a conditional access system may act as a toll bridge for access to services thereby permitting a mechanism for the manufacturer of the set-top box to collect fees based on use of its set-top box. Similarly, this invention may be implemented within a digital television; for simplicity, the below description of the invention will be directed towards an implementation using a set-top box and a smart card.

In Figure 2, system 30 depicts the general architecture for managing access to a set-top box (STB) 40. Smart Card (SC) 42 is inserted into or coupled to a smart card reader (not shown) of STB 40; an internal bus 45 interconnects STB 40 and SC 42 thereby permitting the transfer of data therebetween. Such smart cards include ISO 7816 cards complying with National Renewable Security Standard (NRSS) Part A or PCMCIA cards complying with NRSS Part B. Conceptually, when such a smart card is coupled to a smart card reader, the functionality of the smart card may be considered to be a

part of the functionality of the set-top box thus removing the "boundaries" created by the physical card body of the smart card.

STB 40 can receive services from a plurality of service providers (SPs), such as a broadcast television SP 50, a cable television SP 52, a satellite system SP 54, an internet SP 56, and an electronic event guide SP 58. Certificate authority (CA) 75 is not directly connected to either the service providers or STB 40 but issues digital certificates and public and private key pairs which are used as explained below. A set-top box public key is provided to the manufacturers of the devices and is stored therein before the product is shipped to the consumer. It is within the scope of this invention that the role of certificate authority 75 may be performed by the service providers in collaboration with the manufacturer of the STB 40. Billing system 70 is utilized to manage the user's accounts; updated information is provided as user's make arrangements to purchase additional services and as these services are consumed or used.

The general architecture of system 30 lends itself to achieving the goal of providing a vehicle for the manufacturer of the set-top box to collect a fee based on the consumer's use of the box to access an event. One adaptation of the general architecture would be to utilize a common conditional access and billing system encompassing all manufacturers and service providers. A problem with such an adaptation is that it may be difficult to obtain consensus amongst the various service providers and manufacturers of the set-top boxes. Another problem is that all the events would be encrypted using the public key of STB 40 and decrypted in SC 42 utilizing a

stored private key of STB 40; thus if the private key were to be compromised the security of the entire system would collapse.

The conditional access system of the present invention, which overcomes the above problems, will be described in relation to system 300 as shown in Figure 3. This conditional access system is based on authentication of the service provider communicating with STB 400 prior to purchasing a broadcast event from the service provider. In one embodiment of this conditional access system a combination of both an asymmetric key system (i.e., public-key system) and a symmetric key system is used. However, this invention is not limited to such an embodiment requiring symmetric keys as described below.

Symmetric key cryptography involves the use of the same algorithm and key for both encryption and decryption. The foundation of public-key cryptography is the use of two related keys, one public and one private. The private key is a secret key and it is computationally unfeasible to deduce the private key from the public key which is publicly available. Anyone with a public key can encrypt a message but only the person or device having the associated and predetermined private key can decrypt it. Similarly, a message can be encrypted by a private key and anyone with access to the public key can decrypt that message. Encrypting messages using a private key may be referred to as "signing" because anyone holding the public key can verify that the message was sent by the party having the private key. This may be thought of as being analogous to verifying a signature on a document.

A digitally signed message is a message sent in the clear (i.e., unencrypted) having a signature attached thereto. The attached signature is produced by encrypting either the message itself or a digest of the message; a digest of the message is obtained by hashing the message. (Hashing involves subjecting the message to a one-way hashing algorithm, such as MD5 developed by Ron Rivest or SHA-1 developed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) prior to encrypting the message.) Thus the recipient of the signed message can verify the source or origin of the message. (In comparison, a public key certificate or digital certificate is a message, containing a public key of the sending device, sent in the clear having a signature attached thereto.) Unilateral authentication of a service provider connected to the set-top box is achieved by passing such digitally signed messages between the service provider and the set-top box and verifying the signature. Signature verification involves checking the signature by decryption. Particularly, these messages contain at least information associated with the service provider passing the message or the selected event from the service provider and may contain the service provider's public key. These digitally signed messages, which may have signatures created by independent certificate authority 75, are stored by the service provider.

The following nomenclature will be utilized in the below description of the present conditional access system.

KSCpub	SC's public key
KSCpri	SC's private key

KCApub CA's Public Key used to verify signatures

KCApri CA's Private Key used to create signatures

KSPevent A service provider's event key

Conditional access system 300 of Figure 3 includes STB 400 having SC 420 coupled to a card reader (not shown); STB 400 communicates with billing center 700, a plurality of service providers (for simplicity, only one service provider, SP 600, is shown) and EPG 580. As discussed above, the functionality of SC 420 could be integrated into STB 400 and STB 400 could be a digital television. EPG 580 may be a separate service provider wherein electronic program guides containing listings of events from a plurality of service providers may be accessed. Alternately, EPG 580 may represent only a listing of events from a single service provider.

EPG 580 has a unique digitally signed and encrypted message associated with each event. This message is encrypted by KSCpub and is signed using KCApri, the private key that CA 750 assigned to EPG 580. The encrypted message may include information corresponding to the selected event and an event key, KSPevent.

After STB 400 is activated, SC 420 is coupled to a card reader of STB 400 (not shown), and in response to a user selecting a desired event from EPG 580, EPG 580 downloads the corresponding digitally signed message into STB 400. EPG 580 must be authenticated to ensure that the digitally signed message was received from the desired provider. This authentication involves

decrypting the digital signature in STB 400 using KCApub. KCApub is the public key that CA 750 assigned to EPG 580 and is stored in STB 400. If EPG 580 is not authenticated, STB 400 provides an error indication to the user. Authentication of EPG 580 requires that a pre-existing agreement exists between the electronic guide provider source and the manufacturer of STB 400. This is because without such an agreement CA 750 would not provide KCApri to the source of electronic program guide.

After STB 400 authenticates EPG 580, the encrypted message is passed to SC 420 for decryption. SC 420 decrypts the message using KSCpri, which is stored therein, to obtain the data corresponding to the selected event and the event key. This data may include data relating to channel identity, date and time stamp, event identity, and payment amount. This data is stored in a memory device within SC 420 and is used to update the user account information. The updated account information can be passed to billing center 700 using signed messages.

The event key is retained within SC 420 thereby reducing the possibility of observing the key. The event key is used to descramble, in SC 420, the selected event received from the service provider; SC 420 provides a descrambled program to STB 400. Alternately, the event key could be passed back to STB 400 and used to descramble or decrypt the selected event in STB 400.

If the functionality of the smart card is embedded in the set-top box, the encrypted message would be decrypted within STB 400 and the event information would be stored within the set-top

box. Similarly, the event key would remain in the set-top box and be used to descramble the selected event within STB 400.

System 300', as depicted in Figure 4, shows an alternative exemplary embodiment of the present invention wherein a certification hierarchy may be employed to avoid the certificate authority "signing" every message sent by a service provider. Certificate authority 750' generates a digital certificate for the public key of the service provider. The service provider, then in turn, would generate digitally signed messages using the corresponding private key of the service provider. That is, in response to a user selecting a desired event from EPG 580', EPG 580' downloads a digital certificate and a digitally signed message into STB 400'. The digital certificate is encrypted using KCApri and contains the service provider's public key, KSPpub. The digitally signed message is encrypted by the public key of SC 420', KSCpub, and is signed using the service provider's private key, KSPpri. The encrypted message may include information or data corresponding to the selected event and an event key, KSPevent.

In the same manner as for EPG 580 in the embodiment in Figure 3, EPG 580' must be authenticated. This authentication involves decrypting the digital certificate in STB 400' using KCApub, which is stored therein to obtain KSPpub, and decrypting the digitally signed message in STB 400' using KSPpub.

In another embodiment of the present invention, each unique digitally signed message corresponding to an event listed in the electronic program guide would have an associated encrypted

message. This encrypted message would only contain information related to the event, that is, the event key would not be included. In such an embodiment, public key cryptography may be used to encrypt the broadcast event. The electronic program guide must still be authenticated in STB 400 as described above. However, the decrypted message only contains information corresponding to the selected event. This information is stored and must be used by SC 420 to determine the private key for decrypting the event. In this embodiment utilizing public key cryptography, key transport is not needed.

The present invention has been described in terms of exemplary embodiments in which a single smart card cooperates with a single set-top box to manage access to a single service provider. However, it is within the scope of this invention to provide a conditional access system which may be extended to permit the smart card to "roam" across (i.e., provide conditional access between) multiple service providers and multiple manufacturers of the set-top boxes.

The robustness of the defined system may be increased by encrypting portions of the event with different keys included in the broadcast stream. Each of these different keys (which are used to decrypt a portion of the event) may be protected using the symmetric key received from the electronic program source.

While the invention has been described in detail with respect to numerous embodiments thereof, it will be apparent that upon reading and understanding of the foregoing, numerous alterations to the described embodiment will occur to those skilled in

the art and it is intended to include such alterations within the scope of the appended claims.

Claims

1. A method for managing access to an event of a service provider, said method comprising:

(a) receiving in a device an electronic list of events from a list provider, said list having a digitally signed message corresponding to each event in said list, each of said digitally signed messages comprise a message encrypted using a second public key and a digital signature created using a first private key;

(b) selecting an event from said list;

(c) receiving in said device said digitally signed message corresponding to the selected event;

(d) authenticating said list provider, using a first public key, in response to said digital signature;

(e) decrypting said message using a second private key to obtain an event key;

(f) receiving from the service provider said selected event, said selected event being scrambled using said event key; and

(g) descrambling said selected event using said event key to provide a descrambled event.

2. The method of Claim 1 wherein the steps of decrypting said message, receiving said selected event, and descrambling said selected event are performed in a smart card coupled to the device, said second private and public keys being associated with said smart card and said second private key being stored in said smart card.

3. The method of Claim 2 wherein said message further comprises event information, said event information being decrypted using said second private key.

4. The method of Claim 3 further comprising the step of storing said event information, wherein said step of storing said event information is performed in said removable smart card.

5. The method of Claim 4 wherein said smart card has a card body having a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 and PCMCIA card standards.

6. The method of Claim 5 wherein the step of authenticating comprises decrypting said digital signature in said device to verify the origin of said message.

7. The method of Claim 6 wherein said first public key is stored in said device.

8. The method of Claim 4 wherein said event information comprises channel identification data, event identity data, date and time stamp data, and billing data.

9. The method of Claim 3 further comprising the step of storing said event information, wherein said step of storing said event information is performed in said device.

10. The method of Claim 1 wherein said digital signature, said first public key and said first private key are issued by an independent certificate authority and are associated with said list provider.

11. The method of Claim 10 wherein said device is a digital television.

12. The method of Claim 10 wherein said device is a set-top box.

13. The method of Claim 4 wherein said event information is used within said device to update said user's account information.

14. The method of Claim 13 wherein said event information is downloaded to an independent billing center to update a user's account information.

15. A method for managing access between a device having a smart card coupled thereto and a service provider, said device performing the steps of:

(a) receiving an electronic program guide from a guide provider, said guide having a digitally signed message corresponding to each event in said guide, each of said digitally signed messages comprise a message encrypted using a public key of the smart card and a digital signature created using a private key of said guide provider;

(b) selecting an event from said guide;

(c) receiving said digitally signed message corresponding to the selected event;

Article 34 Amdt

(d) authenticating said guide provider by decrypting said digital signature using a public key of said guide provider, said guide public key being stored in said device;

(e) passing said message to a smart card coupled to the device;

(f) decrypting said message using a private key of the smart card to obtain event information and a symmetric key, said smart card private key being stored within the smart card;

(g) storing said event information in the smart card and updating account information based on said event information;

(h) receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and

(i) descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event.

16. The method of Claim 15 wherein the device is a set-top box.

17. The method of Claim 15 wherein the device is a digital television.

18. A method for managing access between a device having a smart card coupled thereto and a service provider, said device performing the steps of:

(a) receiving an electronic program guide, said guide having a digital certificate and a separate message corresponding to each event in said guide, each of said digital certificates being encrypted using a first private key of said guide, said separate message being encrypted using a public key of the smart card and having an associated digital signature created using a second private key of said guide;

(b) selecting an event from said guide;

(c) receiving said digital certificate, said message and said digital signature corresponding to the selected event;

(d) authenticating said guide provider by decrypting said digital certificate using a first public key of said guide to obtain a second public key of said guide, and decrypting said digital signature using said second guide public key, said first guide public key being stored in the device;

(e) passing said message to said smart card;

(f) decrypting said message using a s private key of the smart card to obtain event information and a symmetric key, said smart card private key being stored within the smart card;

(g) storing said event information in the smart card and updating account information based on said event information;

(h) receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and

(i) descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event.

19. The method of Claim 18 wherein the device is a set-top box.

20. The method of Claim 18 wherein the device is a digital television.

Abstract of the Disclosure

A method for managing access to a scrambled event, selected from an electronic program guide, of a service provider (including broadcast television networks, cable television networks, digital satellite systems, and internet service providers). Access to the event is only achieved if the descrambling key is obtained from a digitally signed message associated with the event in the electronic program guide. Authentication of the electronic program guide provider involves decrypting the digital signature using a public key of the guide provider.

09/445133

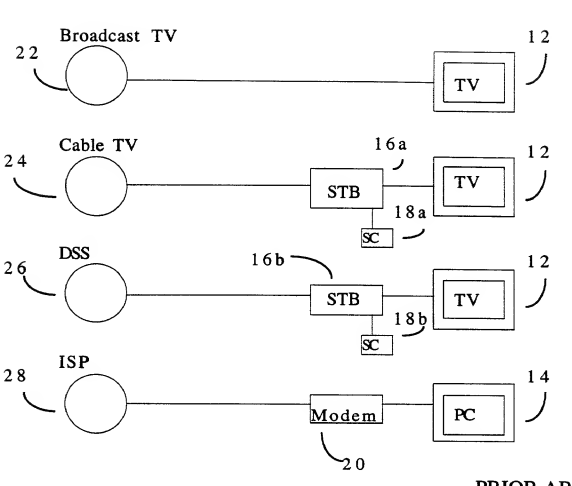


Fig 1

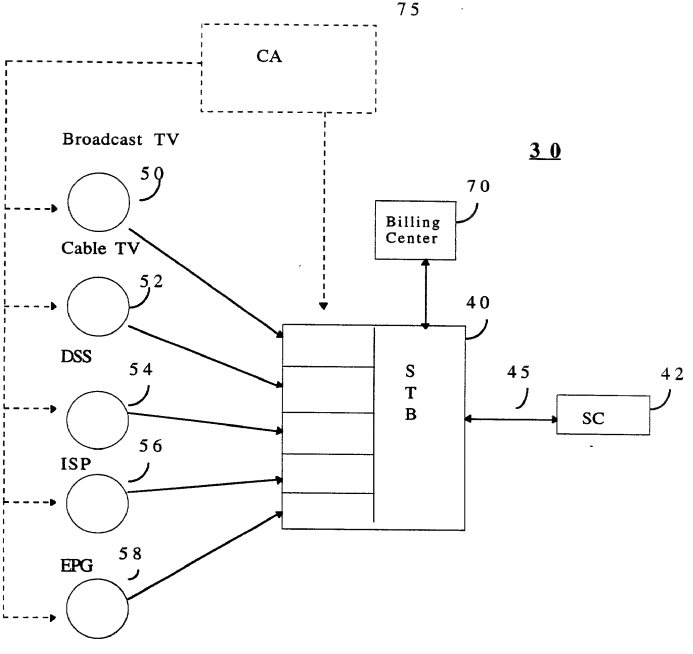

75
CA
Broadcast TV
30
50
70
Billing Center
Cable TV
52
40
DSS
54
S
T
B
45
42
SC
ISP
56
EPG
58

Fig 2.

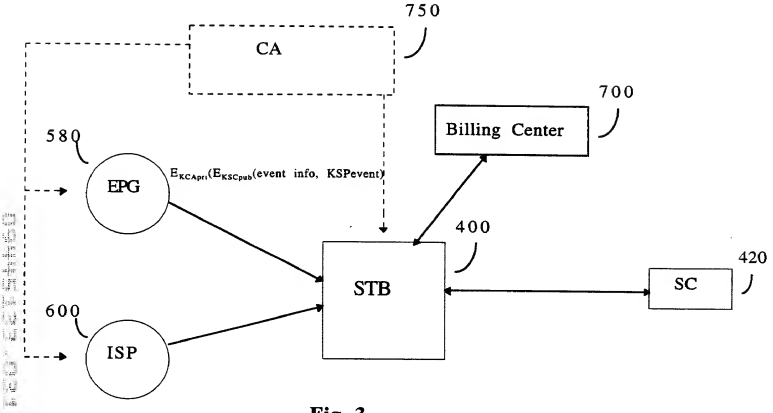


Fig 3.

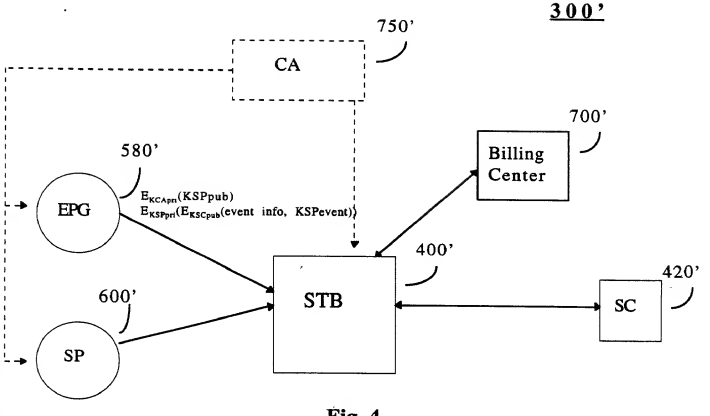
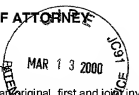

300'
750'
CA
700'
Billing Center
580'
EPG
$E_{KCApri}(KSPpub)$
$E_{KSPpri}(E_{KSCpub}(event\ info,\ KSPevent))$
400'
420'
600'
STB
SC
SP

Fig 4.

RCA 88,674

DECLARATION AND POWERS OF ATTORNEY



As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled
GLOBAL CONDITIONAL ACESS SYSTEM FOR BROADCAST SERVICES
the specification of which was filed on **12/3/99** as Application Serial No. **09/445,133** and was amended on _____
or, if not identified here by filing date and serial number, is attached hereto.

I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with 37 CFR 1.56.

I hereby claim foreign priority benefits under 35 USC 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate by me or my representatives or assigns for this invention having a filing date before that of the application on which priority is claimed.

Application No. _____ in _____ on _____ priority claimed [ ] Yes [ ] No
Application No. _____ in _____ on _____ priority claimed [ ] Yes [ ] No

I hereby claim the benefit under 35 USC 119(e) of any United States provisional application(s) as listed below.

Application No. **60/048,852** Filed **6/6/97**
Application No. Filed

I hereby claim the benefit under 35 USC 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of 35 USC 112, I acknowledge the duty to disclose material information as defined in 37 CFR 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application

Serial No. PCT/US98/11634 Filed 6/5/98 [ ] patented [X] pending [ ] abandoned

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 USC 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint, individually and collectively, the following as my/our attorney or agent with full power of substitution and revocation, to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected therewith:

3

Joseph S. Tripoli Registration No. 28,040 and
Robert D. Shedd Registration No. 36,269 and
David T. Shoneman Registration No. 39,371

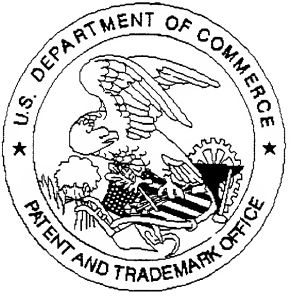
PLEASE ADDRESS ALL
COMMUNICATIONS TO: **JOSEPH S. TRIPOLI**
PATENT OPERATIONS
THOMSON MULTIMEDIA LICENSING, INC.
P. O. Box 5312
PRINCETON, NEW JERSEY 08543-5312

1

Sole or Joint Inventor (1)	Ahmet Mursit Eskicioglu (Type or Print)	Ahmet Mursit Eskicioglu (Signature in Full. No initials.)
Citizenship	Turkey	Date 3/6/00
Post Office Address	8235 Lakeshore Trail No. 124, Indianapolis, IN 46250 USA	
Residence	Same as above	
Sole or Joint Inventor (2)	(Type or Print)	(Signature in Full. No initials.)
Citizenship		Date
Post Office Address		
Residence	Same as above	
Sole or Joint Inventor (3)	(Type or Print)	(Signature in Full. No initials.)
Citizenship		Date
Post Office Address		
Residence	Same as above	

United States Patent & Trademark Office

Office of Initial Patent Examination -- Scanning Division



Application deficiencies were found during scanning:

☐ Page(s) 20 of Specification were not present for scanning.
(Document title)

☐ Page(s)_____ of _____ were not present for scanning.
(Document title)

☐ Scanned copy is best available.